

# Analyzing Safety in Collaborative Cyber-Physical Systems: A Platooning Case Study

Manzoor Hussain, Nazakat Ali, Youngjae Kim, and Jang-Eui Hong

Department of Computer Science, Chungbuk National University

Cheongju, Republic of Korea

[hussain@selab.cbnu.ac.kr](mailto:hussain@selab.cbnu.ac.kr)



## Manzoor Hussain

He is currently pursuing the Integrated (M.S. leading to Ph.D.) degree with the Department of Computer Science, School of Electrical and Computer Engineering, Chungbuk National University, South Korea. He worked as a Software Developer with GIKI, Pakistan.

### Research Interests:

- Software engineering
- Deep learning,
- Cyber-physical systems
- Autonomous system's safety.
- Deep reinforcement learning

# Software Engineering Laboratory, Chungbuk National University Korea

## Intelligent CPS research group

Prof. JANG-EUI HONG (Ph.D.)

Research Interest: *include software quality, embedded software architecture, low-energy software development, and software system safety.*

Dr. NAZAKAT Ali (Ph.D.)

Research Interest: *software requirements engineering, data mining, ontology, software architecture, software process improvement, DevOps, software quality, system safety, system of systems, and cyber-physical systems.*

YOUNGJAE KIM

Research Interests: *Cyber Physical Systems, safety, Simulation, autonomous vehicle, and Platoon driving.*

# Topics to be discussed

- 1 Introduction
- 2 Motivation
- 3 Related Work
- 4 Proposed Approach
- 5 FPTG, FPG, and FBTG
- 6 Safety Verification
- 6 Conclusion

# Introduction

- Collaborative Cyber-Physical Systems (CCPS)
  - Controlled, reliable, connected and complex system
  - Collaborate
  - Can perform complex task
- Cyber Physical Systems may face unexpected behavior
  - Unintended behavior of failure free system due to performance limitation
  - Lack of robustness
    - Environmental variabilities
  - Lack of composite hazard analysis
    - Lack of fault traceability
  - Insufficient situational awareness
- Single CPS's safety can be insured by
  - ISO 26262
  - IEC61508

# Introduction

- Safety of CCPS becomes challenging tasks
  - Complex, diverse, variable and uncertain operational environment
    - e.g., autonomous platooning system
      - Environmental uncertainties such as Fog, rain and snow
      - Infrastructural uncertainties such as black ice on road etc.
  - CCPS are massively interconnected
    - Single fault can activate many other fault in other collaborating systems.
- We present an enhanced fault traceability approach
  - Composite hazard analysis
  - Content relationship among hazard analysis artifacts
    - Fault Tree Analysis (FTA), Failure Mode and Effect Analysis(FMEA) and Event Tree Analysis (ETA)
  - Fault traceability Graphs
    - Fault Traceability and Propagation Graph (FPTG)
    - Fault Propagation Graph (FPG)
    - Fault Back Traceability Graph (FBTG)
  - Case Study: Autonomous Platooning System

# Motivation

## Introducing the enhanced fault traceability techniques

- Traceability Graphs
  - Single hazard analysis technique is not sufficient for CCPS
  - Composite hazard Analysis of CCPSs
  - Content relationships among hazard analysis artifacts
  - FPTG, FPG, FBTG
    - Fault Route
    - Source of Fault
    - Propagation Scope
    - Impact of fault of on other system
    - Safety guard
- Safety verification of Platooning systems
  - VENTOS Simulator
  - Hazardous scenarios *i.e., fog, rain, and black snow*

### Composite Hazard Analysis

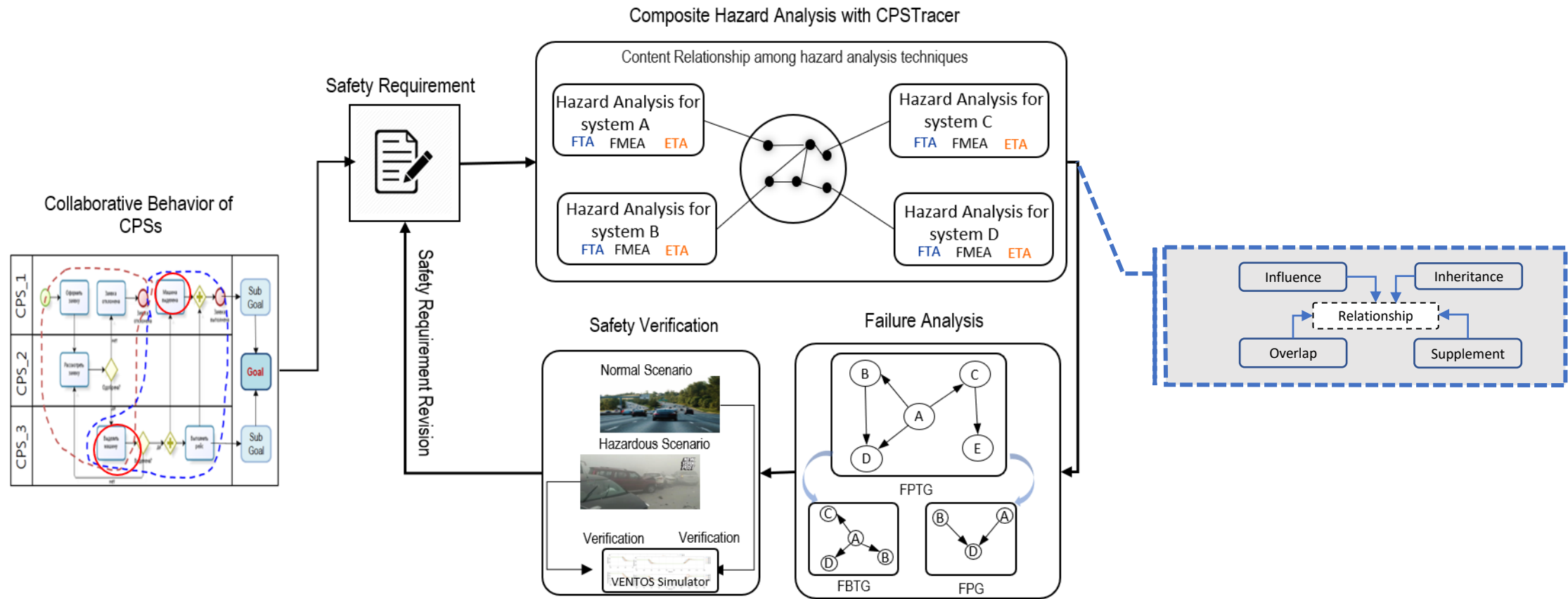
- Composite Hazard Analysis Technique
  - FTA
  - FMEA
  - ETA
- Content Relationships
  - Influence Relationship
  - Inheritance Relationship
  - Overlap Relationship
  - Supplement Relationship

# Related Work

- **Ali et al.** Presents an approach that can model the uncertainties that collaborative CPSs may face during their operation. They extended the traditional FTA, FMEA, ETA to model the variabilities and uncertainties in CPSs. [2020]
- **Daneth et al.** A domain-specific language (CyPhyML+) was to identify the interaction component and their uncertainties in collaborative CPSs. [2019]
  - The primary objective of this approach was to present the safety component and identifying unknown component interaction in CPSs ensuring safety
- **Naufal et al.** proposed a conceptual framework called **A2CPS (autonomous CPSs)** aiming to design and implement an autonomous supervision and control system. [2018]
  - Purpose of this approach was to reduce vehicle collision with resilient safety measure at run time
- **Medawar et al.** discussed the role of the run-time manager in SafeCOP to ensure continuous safety in truck platooning. [2017]
  - The authors first specify the safety contracts based on the safety analysis of the local system as well as the cooperative safety function.
- **Zhang et al.** proposed a taxonomy that can be translated under the uncertainty of the predictive model. [2016]
  - A self-healing model is proposed to ensure the sustainable safety of the CPSs.



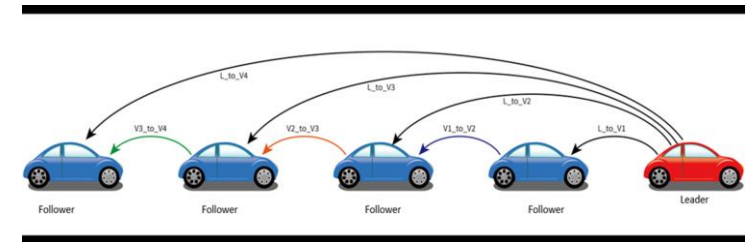
# Proposed Approach



# Safety Analysis of Platooning System (A collaborative CPS)

## • Platooning System

- The movement of vehicle group collaborates to reduce the inter-vehicle distance and creates synergy. The front vehicle called leader, and the following car called follower.
  - Better usage of road infrastructure i.e., can fit more vehicles on the road
  - Improve energy efficiency by reducing the aerodynamic drag
  - Reduce emission
  - Full consumptions

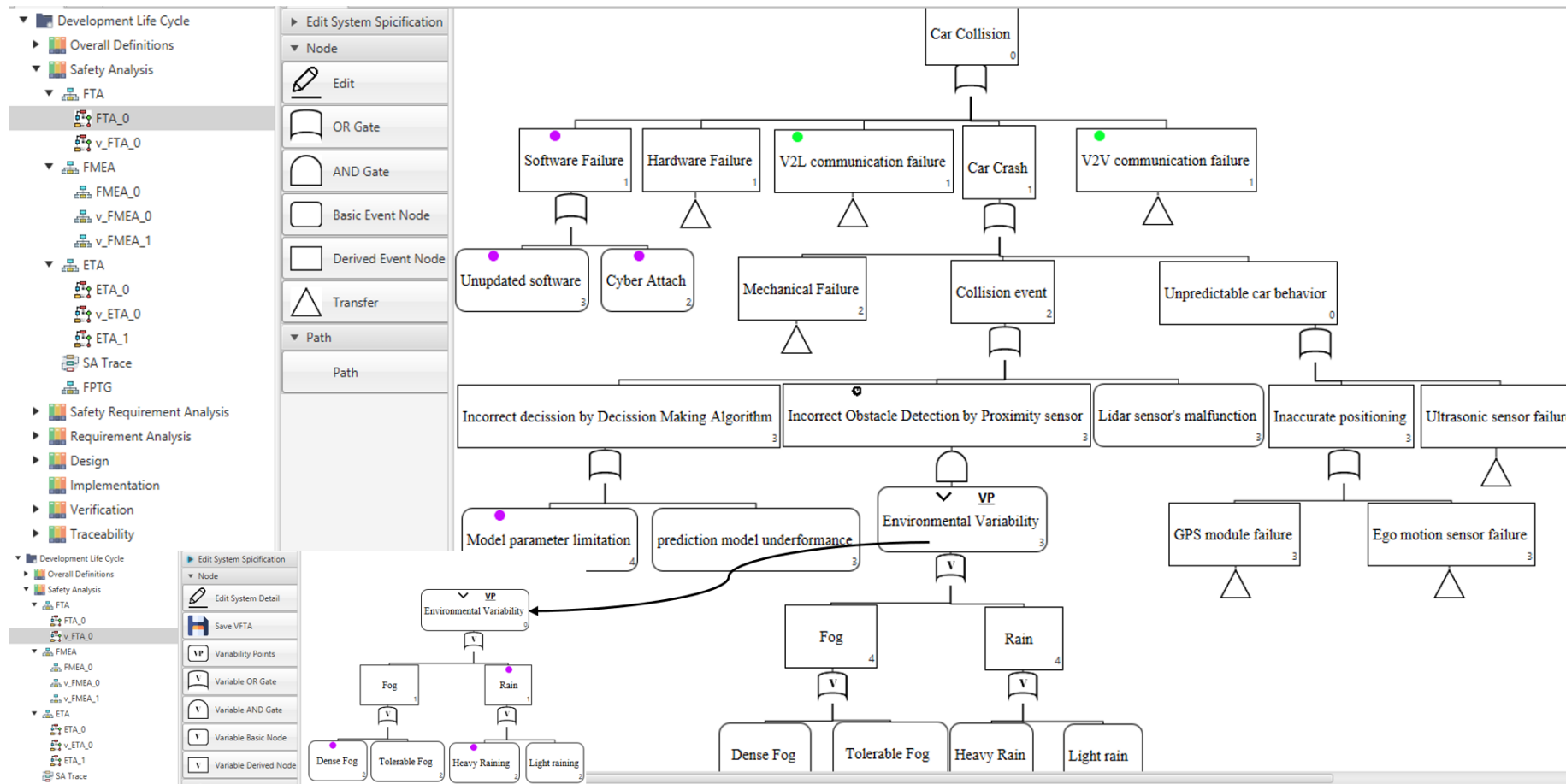


Example of Platooning system

## • However,

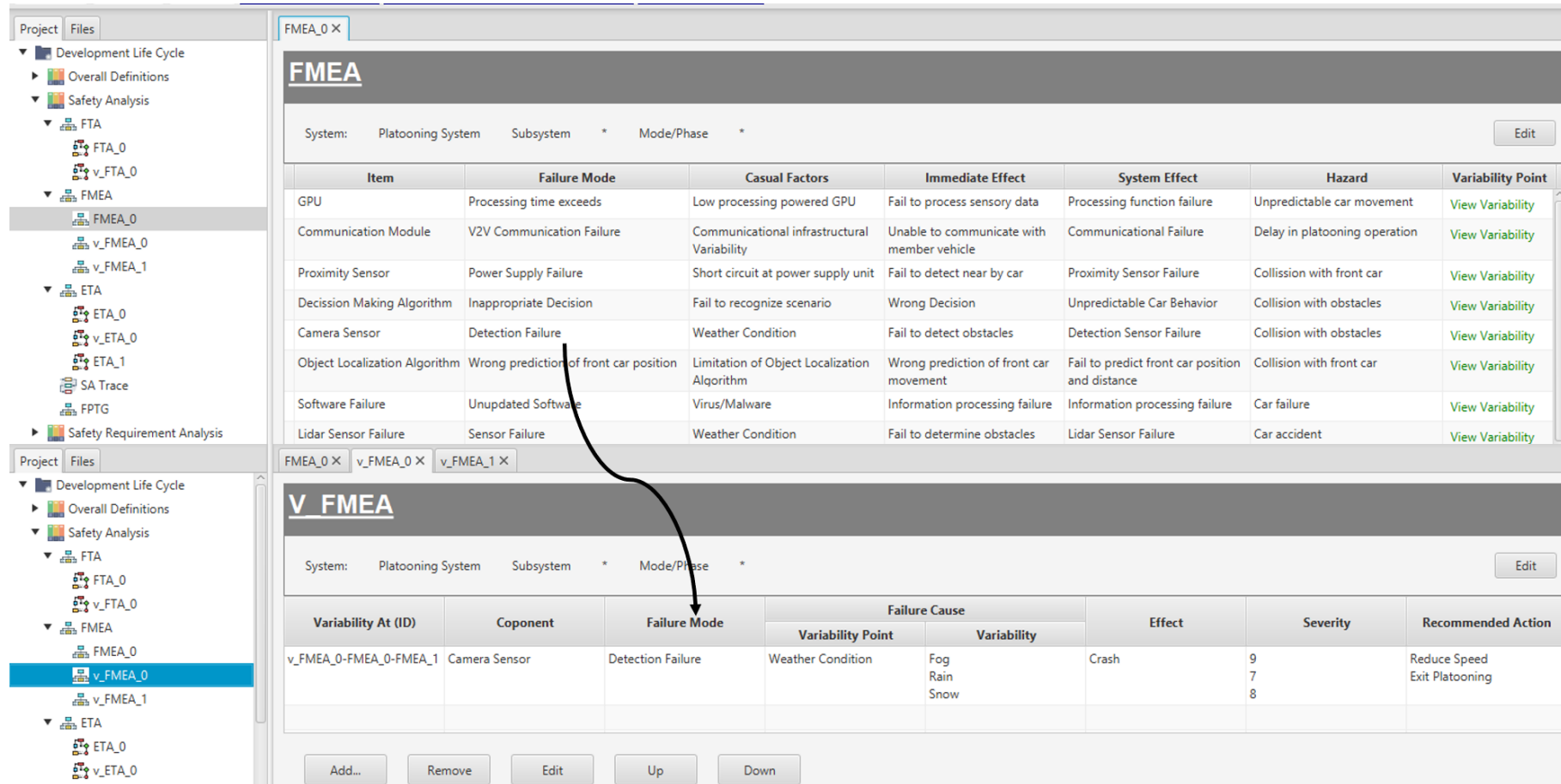
- Reducing the inter-vehicle distance also leads to creating safety concerns in vehicles participating in the platooning.
- The safety of collaborative CPSs can be ensured by analyzing the safety of the system considering the potential uncertainties.
  - To identify the potential hazards, analyze the faults, and measurement of possible damage.

# Composite Hazard Analysis of Platooning CPS- Fault Tree Analysis



Fault Tree Analysis of The Platooning Systems

# Composite Hazard Analysis of Platooning CPS- Failure Mode Effect Analysis



**FMEA**

System: Platooning System    Subsystem: \*    Mode/Phase: \*

Item	Failure Mode	Casual Factors	Immediate Effect	System Effect	Hazard	Variability Point
GPU	Processing time exceeds	Low processing powered GPU	Fail to process sensory data	Processing function failure	Unpredictable car movement	<a href="#">View Variability</a>
Communication Module	V2V Communication Failure	Communicational infrastructural Variability	Unable to communicate with member vehicle	Communicational Failure	Delay in platooning operation	<a href="#">View Variability</a>
Proximity Sensor	Power Supply Failure	Short circuit at power supply unit	Fail to detect near by car	Proximity Sensor Failure	Collision with front car	<a href="#">View Variability</a>
Decision Making Algorithm	Inappropriate Decision	Fail to recognize scenario	Wrong Decision	Unpredictable Car Behavior	Collision with obstacles	<a href="#">View Variability</a>
Camera Sensor	Detection Failure	Weather Condition	Fail to detect obstacles	Detection Sensor Failure	Collision with obstacles	<a href="#">View Variability</a>
Object Localization Algorithm	Wrong prediction of front car position	Limitation of Object Localization Algorithm	Wrong prediction of front car movement	Fail to predict front car position and distance	Collision with front car	<a href="#">View Variability</a>
Software Failure	Unupdated Software	Virus/Malware	Information processing failure	Information processing failure	Car failure	<a href="#">View Variability</a>
Lidar Sensor Failure	Sensor Failure	Weather Condition	Fail to determine obstacles	Lidar Sensor Failure	Car accident	<a href="#">View Variability</a>

**V FMEA**

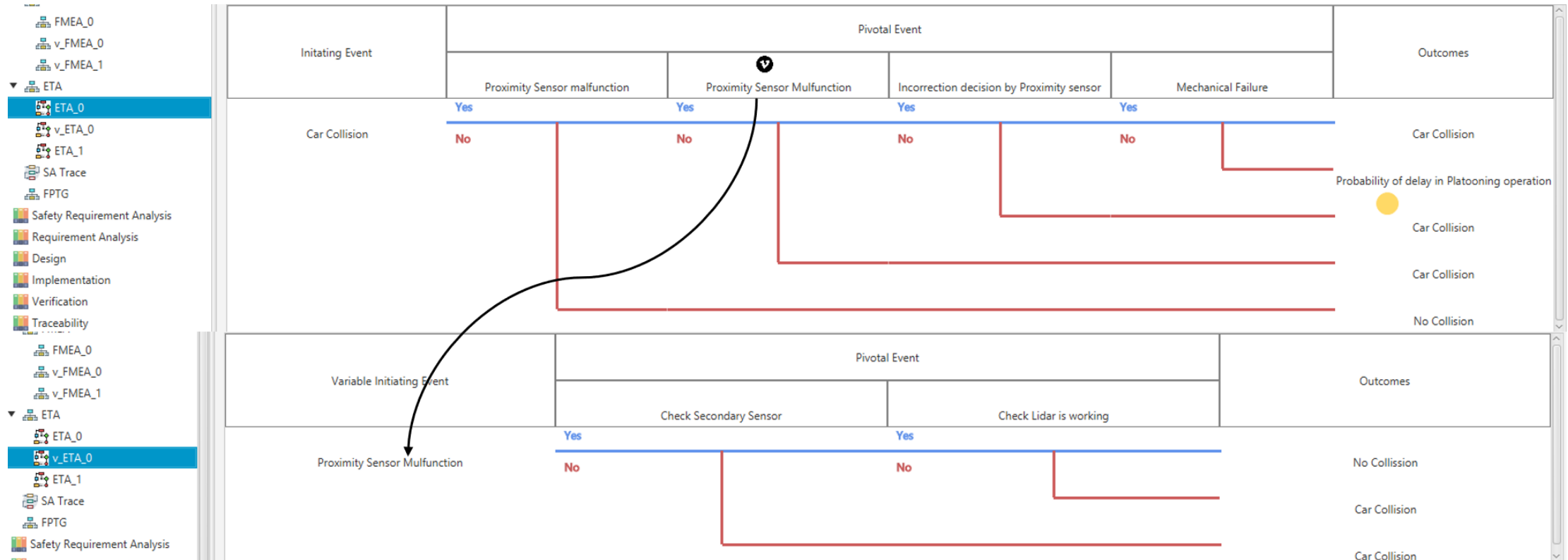
System: Platooning System    Subsystem: \*    Mode/Phase: \*

Variability At (ID)	Copenent	Failure Mode	Failure Cause		Effect	Severity	Recommended Action
			Variability Point	Variability			
v_FMEA_0-FMEA_0-FMEA_1	Camera Sensor	Detection Failure	Weather Condition	Fog Rain Snow	Crash	9 7 8	Reduce Speed Exit Platooning

Buttons: Add... Remove Edit Up Down

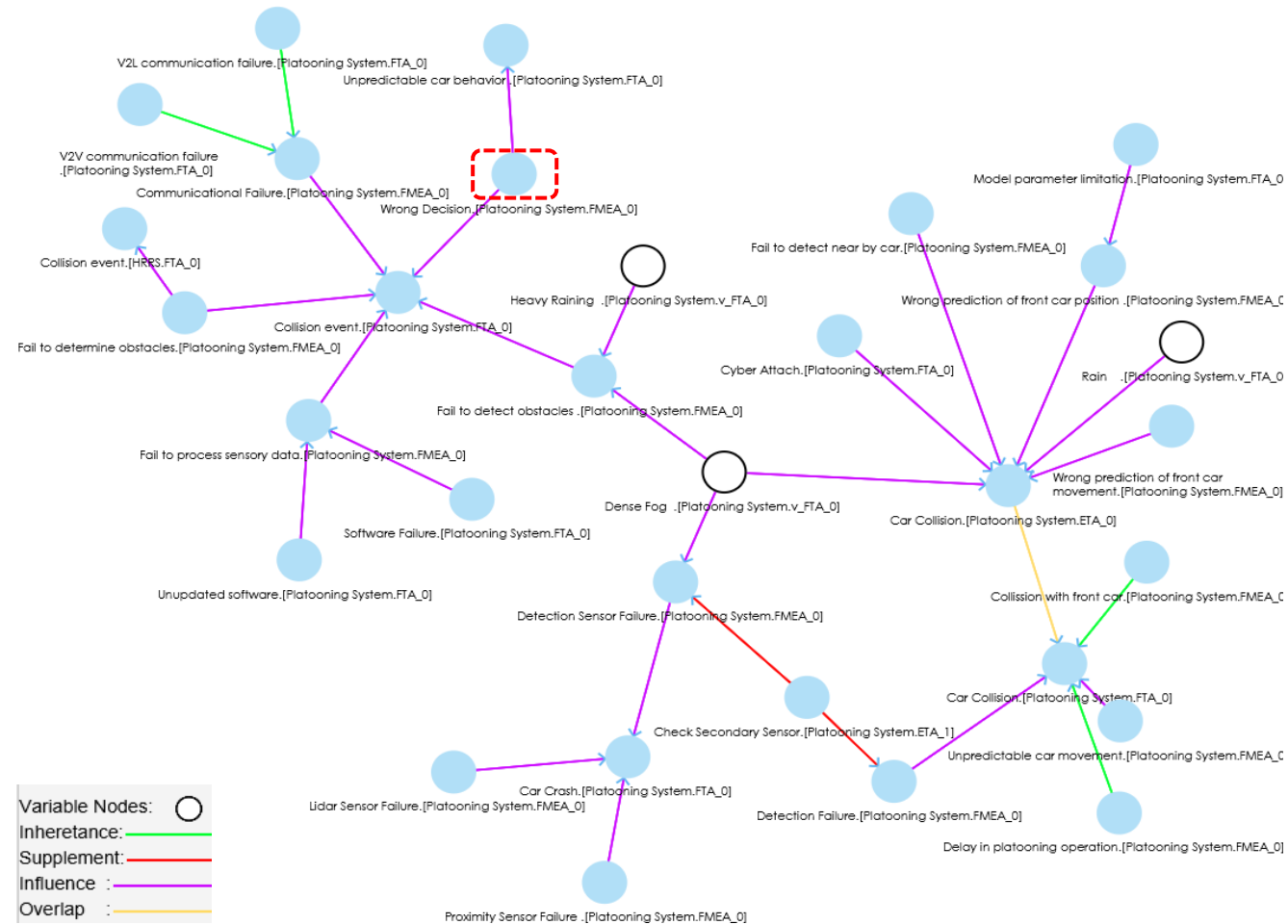
Failure Mode Effect Analysis of The Platooning Systems

# Composite Hazard Analysis of Platooning CPS- Failure Mode Effect Analysis



Event Tree Analysis of The Platooning System

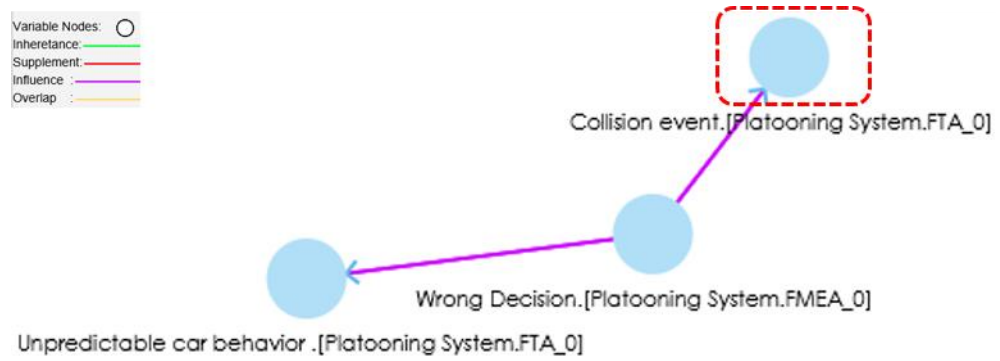
# Safety Analysis of Platooning System with FPTG



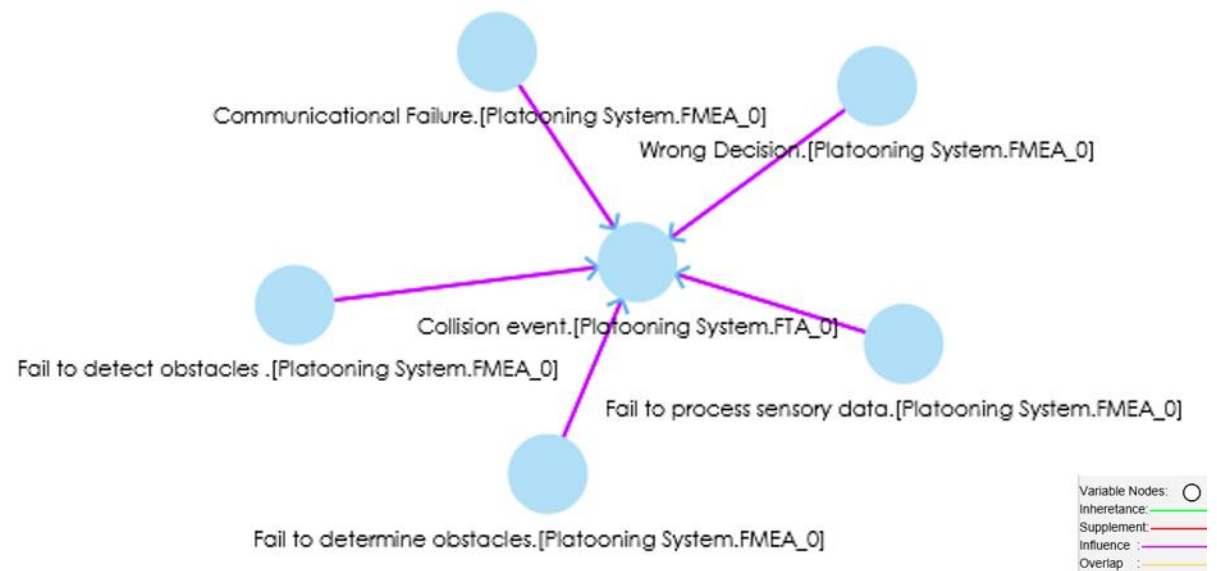
Fault Propagation Traceability Graph of the Platooning Systems

# Safety Analysis of Platooning System with FPG and FBTG

Variable Nodes: ○  
 Inheritance: —  
 Supplement: —  
 Influence: —  
 Overlap: —



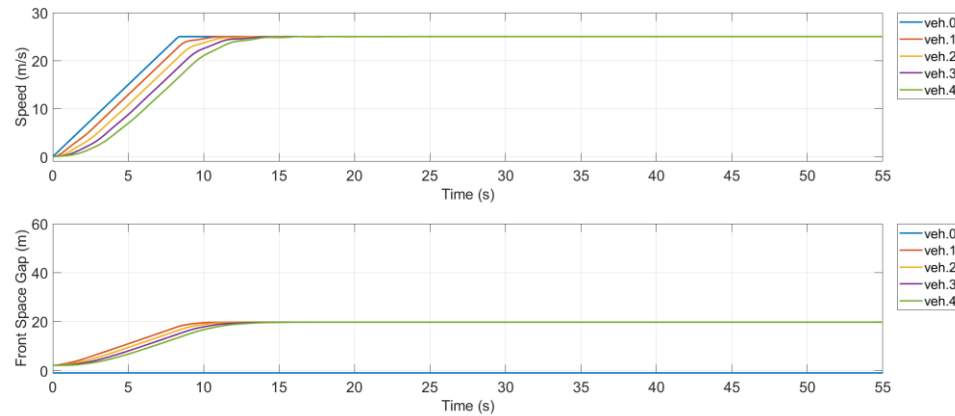
Fault Propagation Graph of the Platooning Systems



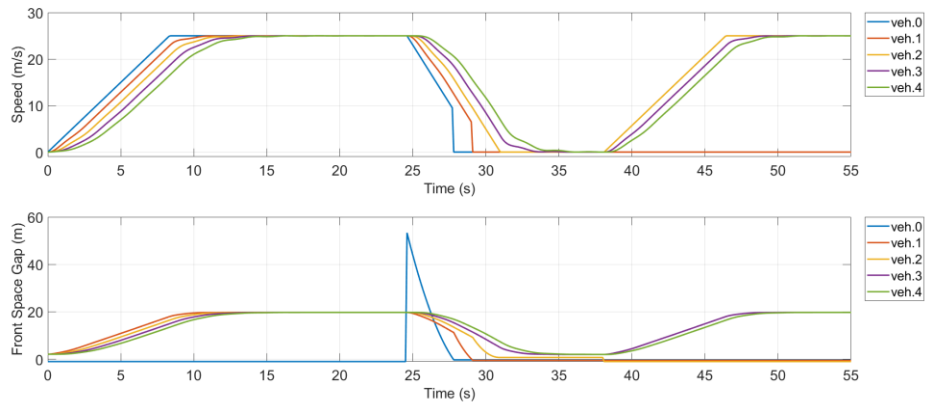
Variable Nodes: ○  
 Inheritance: —  
 Supplement: —  
 Influence: —  
 Overlap: —

Fault Back Traceability Graph of the Platooning Systems

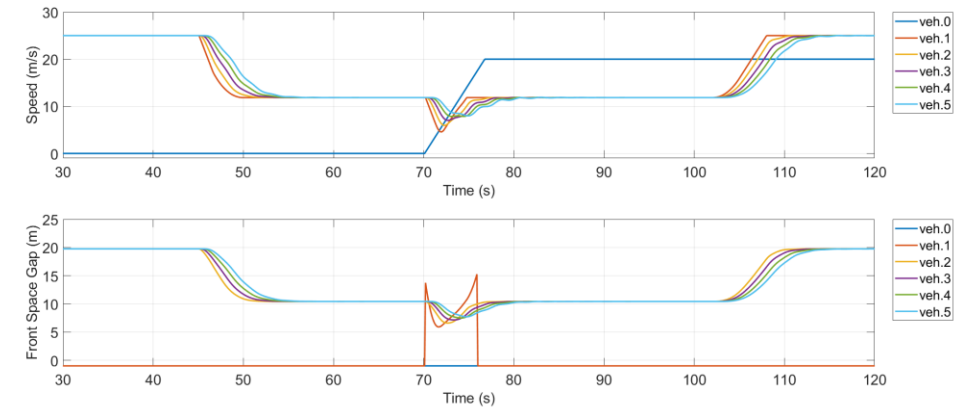
# Safety Verification



Speed and inter-vehicle distance for the normal scenario.



Speed and inter-vehicle distance for the hazardous scenario.



Speed and inter-vehicle distance for safe scenario



# Conclusion

- Collaborative Cyber-Physical Systems (CCPS)
  - Complex and massively in inter-connected
  - Unexpected behavior in CCPSs may comes due to diverse, variable and uncertain operational environment
- Safety of CCPS is challenging task due to
  - Complex, diverse, variable and uncertain operational environment
    - Environmental uncertainties such Fog, rain and snow
    - Infrastructural uncertainties such as black ice on road etc.
  - CCPS are massively interconnected
    - Single fault can activate many other fault in other collaborating systems.
- We present an enhanced fault traceability approach
  - Composite hazard analysis
  - Content relationship among hazard analysis artifacts
    - Fault Tree Analysis (FTA), Failure Mode and Effect Analysis(FMEA) and Event Tree Analysis (ETA)
  - Fault traceability Graphs
    - Fault Traceability and Propagation Graph (FPTG)
    - Fault Propagation Graph (FPG)
    - Fault Back Traceability Graph (FBTG)
  - We verified our approach by analyzing the Autonomous Platooning System in VENTOS Simulations

# Questions and Discussion

Hussain@selab.cbnu.ac.kr